UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/456,794	12/08/1999	JAY C. CHEN	34581/CAG/C718	6924

7590 03/24/2004

McDermott Will & Emery
Attn: Craig A. Gelfound
2049 Century Park East
34th FL
Los Angeles, CA 90067-3208

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2137	24

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/456,794	CHEN, JAY C.	
	Examiner	Art Unit	
	Douglas J. Meislahn	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *81-116* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *81-116* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 June 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the request for reconsideration filed 29 December 2003.

Response to Arguments

2. Applicant's arguments filed 29 December 2003 have been fully considered but they are not persuasive.

3. Applicant opines that the objection to the claims is uncalled for. Elements 1-10 are not labeled. Even when the drawings are reviewed, these elements' meaning is unclear. The same goes for element 1180.

4. Applicant argues that the claims and the rejection are different because the Woo-Lam protocol (used in the rejection) uses three entities while the claims use two entities (1A). While correct, the rejection has provided a secondary reference and motivation for embodying the functions of one of the three Woo-Lam entities, Trent, in one of the remaining entities, Bob. Applicant has not addressed this reasoning, and hence this argument is unpersuasive.

5. Applicant's argument 1B focuses on an apparently unfortunate phrase used in the previous rejection. Specifically, the previous action mentioned, "external generation of the session key". External generation of an encryption key is generation of an encryption key by an entity that is not going to use the key. The session key used in Woo-Lam is generated by Trent, who creates the key not for his personal use, but only to send it to another entity. As applicant says, Trent is not external to the Woo-Lam system. Applicant further opines that

removing Trent would render Woo-Lam inoperable. By itself, this is correct; but the rejection, while removing the entity Trent, moves Trent's functionality into one of the remaining entities, as is suggested by the prior art. Therefore, applicant's argument that the removal of Trent renders the rejection nonsensical is unpersuasive.

6. With respect to applicant's argument 2A, the first two steps of the Woo-Lam protocol, which pertain to acquiring a public key, are immaterial to the claims. Their existence does not constitute grounds for allowance. Applicant seems to want to imply that these two steps are contrary to public key acquisition steps of the current invention. However, the claims are silent as to how the public key is acquired. It is entirely possible that applicant's two-party system actually uses a third party to secure the public key. As such, any argument that the method in which the Woo-Lam protocol acquires a public key differentiates it from the claims is unpersuasive.

Applicant also quotes a statement made by the examiner reciting the steps of the Woo-Lam protocol. It is unclear how the examiner's reiteration of steps of the Woo-Lam protocol distinguishes the claims from the rejection. Applicant concludes this section by intoning that the three-party Woo-Lam protocol is different from the instant invention. That the examiner agrees is evidenced by the inclusion of other references in the rejection, where the rejection teaches all of the elements of the claims to which it is applied.

7. Argument 2B speculates as to the result of the combination of the Woo-Lam protocol and Ginzboorg et al. Since there is a third reference in the rejection, this exercise is moot and hence an unpersuasive argument.

8. Applicant interprets the security flaws in Woo-Lam as meaning that the instant invention is "superior". But is it? One of the security concerns of Woo-Lam is that Trent is dishonest and will use the session keys that he generates illicitly. But what if Trent is actually benevolent and Bob is dishonest, sending Alice weak keys for one mischievous reason or another. Is the instant invention still "superior" to the Woo-Lam protocol? Blanket assertions about the relative strengths of two security systems are inappropriate because the relative merits of two such systems are rarely, and in the current case not at all, comparable because the environment in which the systems exist moderates their effectiveness. As such, this argument is unpersuasive. Furthermore, the rejection is made of a combination of three references, the combination of which needs to be shown to lack elements of the claims for the claims to be allowable.

9. Argument 3B suffers from applicant's misinterpretation of external generation of an encryption key. The examiner has never implied or stated that Trent is outside of the system of the Woo-Lam protocol. Applicant again notes that the instant invention does not use three parties. However, the claims do not bar a third party from assisting in some aspects of the transaction, such as providing public keys.

10. The examiner does not see how argument 3C distinguishes the prior art from the claimed invention. There are no algorithms dictating session key

generation in either the claims or the cited art. The rejection clearly presents grounds for the rejection of the instant claims. As such, this argument is unpersuasive.

11. Applicant opines, in argument 3D, that the Woo-Lam protocol's use of Trent to procure public keys distinguishes the rejection from the instant claims. The instant claims are silent as to the acquisition of the public keys. As such, Trent's providing the public keys in Woo-Lam does not differentiate the current claims from the rejection.

12. Argument 4A is directed towards a quotation, made by the examiner, that recaps the rejection of claim 81. The argument is that the recap incorrectly states the combination of Schneier (which has taught both Woo-Lam and a second protocol) and Ginzboorg et al. Applicant's conclusion is flawed because it is based on the arguments that have been rebutted in the above paragraphs.

13. In argument 5A, applicant opines that the claims do not use a certificate. The claims are silent with respect to certificates. As such, their inclusion in the rejection does not differentiate the claims from the prior art.

14. In argument 5B, applicant notes that both Bob and Trent already have other ways to get Alice's public key. However, sending the key to Bob would let him verify that he gets the correct key from Trent. As such, there is no basis for applicant's opinion that Bob would not accept Alice's certificate. Implicit to this argument is the conjecture that the instant invention does not need certificates to verify public keys. This is not supported by the claims. Nor is it likely given the current state of the art. As such, this argument is unpersuasive. By "Alice's first

message", the examiner means the first communication between Alice and a second party, be it Trent, Bob, or another entity.

15. Applicant presents a summary in argument 5C. This argument is unpersuasive because it is a summary of arguments that have been refuted in the above paragraphs. The argument also should say that the rejections are based on Ginzboorg et al. in view of Schneier, not Schneier in view of Ginzboorg.

16. Argument 6A is flawed because it is based on the validity of applicant's previous arguments, all of which have been rebutted.

17. In response to applicant's argument (6Ba) that Thompson et al. is concerned with piggybacking and transmission efficiency, the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985).

18. With respect to argument 6Bb, the elements that would differentiate Thompson et al. from the instant invention are not claimed. Therefore the argument is unpersuasive.

19. With respect to applicant's conclusion, the above discussion of applicant's arguments, the claims, and the prior art makes clear that the elements of the claims are rendered obvious by the rejection.

20. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably

distinguishes them from the references. In this case, this is a particular difficulty because the instant invention is largely directed to two entities, but a hard limit to those two would present many security problems, such as eradicating the best-known way to reliably authenticate public keys.

Drawings

21. The drawings are objected to because elements 1-10 in figure 2 and 1180 in figure 12 are not labeled. Correction is required. Numbers do not count as labels.

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. Claim 81 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al. (6240091) in view of Schneier.

In lines 51-67 of column 7, Ginzboorg et al. present a smart card that includes, among other pieces of data, the public key of a second party. As evidenced by the abstract and billing system (BS) in figure 3a, Ginzboorg et al. complete a transaction. They do not teach the specific steps of the claims. In describing the Woo-Lam protocol described on page 64, Schneier shows, in step 3, Alice initiating communications with Bob by encrypting a message (Bob's name and a random challenge) with Bob's public key and sending it to him. He

then encrypts Trent's signature, which contains K, with Alice's public key, thereby formatting a key exchange response message, and sends it to her. Alice uses the session key to encrypt Bob's challenge (sent with Trent's signature), and the transaction is completed. Schneier's method provides authentication and a symmetric key. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the teachings of Schneier in Ginzboorg et al.'s system so as to both authenticate parties and in order to provide the parties with a symmetric key.

The Woo-Lam protocol does not task Bob with uniquely generating the session key. In a basic encrypted key exchange protocol where the session key is to be exchanged, described on page 518, step 2, Bob uniquely generates the session key. While not discusses in this session, the benefits of Bob himself generating the session key include minimizing the number of times that the session key is transmitted. Although encrypted, transmitting the session key from Trent to Bob in the Woo-Lam protocol presents a small vulnerability, that being interception and successful illicit decryption of the key. A second vulnerability is that Trent is not actually trustworthy and will maliciously use the session key against Bob and Alice. The benefit of using Trent to generate the session key lies largely in Trent theoretically being trusted as competent in producing session keys. Some cryptanalytic attacks make use of pockets of determinism in key generation. People of ordinary skill in the art know these risks. So, the decision to generate the session key internally or externally should be based on the parties' assessment of the trade-off between the risks.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for Bob to internally generate the session key instead of using a session key received from Trent. By internally making the key, Bob would protect the key from interception and cracking and a dishonest Trent.

24. Claims 82-102 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al. in view of Schneier as applied to claim 81 above, and further in view of Walker et al. (6263438).

Ginzboorg et al. and Schneier teach a smart card that contains a second entity's public key. The smart card and second entity authenticate themselves to one another and agree on a symmetric key. There is no teaching of sending the smart card's public key to the second entity. In lines 38-52 of column 6, Walker et al. teach including digital certificates (which include encrypted forms of an originator's public key) with messages to provide greater assurance. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send a certificate with Alice's first message, as taught by Walker et al., to provide greater assurance.

Step 5 in the Woo-Lam protocol involves the second entity providing a challenge. Schneier teaches signing messages on pages 576 and 577. Ginzboorg et al. also teach signatures in, for example, their abstract. This renders obvious signing all messages sent from one entity to another. See also the additional payment steps shown by Ginzboorg et al.

Ginzboorg et al., Schneier, and Walker et al. do not mention using the symmetric key to protect information, such as account information, a transaction

amount, and sensitive transaction data. Official notice is taken that it is old and well known for a purchaser to encrypt data, including account information, a transaction amount, and sensitive transaction data, with a symmetric key in an electronic transaction in order to prevent that data from being used illicitly. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt transaction data sent between the two entities in order to protect data. Data that need not be protected should not be, thereby reducing cryptographic operations.

Ginzboorg et al., Schneier, and Walker et al. has not mandated that the entities include transaction identifiers with their transaction correspondences. Official notice is taken that it is old and well known to include transaction identifiers assigned by one entity with their transaction correspondences, which helps catalog and identify messages. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include transaction identifiers with their transaction correspondences in order to track messages.

25. Claims 103-116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al., Schneier, and Walker et al. as applied to claim 81 above, and further in view of Thompson et al.

Ginzboorg et al., Schneier, and Walker et al. teach a method for exchanging keys. They do not show the group method of key request. Thompson et al show a method by which changes to a document are recorded. This method entails signing all changes. For the purposes of this discussion, we

will assume that Thompson et al.'s original bill corresponds to applicant's key exchange request. As can be seen in figure 5, the original bill has been signed by the originator and then modified and signed by a second entity, whereby the original bill remains perceptible. The benefit of this is that it allows parties to know exactly what different entities added, as taught in lines 29 and 30 of column 5. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include signatures and recognizable updates as taught by Thompson et al. in Schneier's key exchange requests, thereby piggybacking requests and reducing the total number of transmissions of data.

Different session keys would be the most obvious, as the requesting entities have made no indication of wanting to communicate with each other. However, a scenario where two requesting entities desired the same key so that they could communicate securely is also obvious.

Conclusion

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Douglas J. Meislahn
Examiner
Art Unit 2137

DJM
22 March 2004